T S1/5/1

1/5/1
DIALOG(R)File 347:JAPIO
(c) 2004 JPO & JAPIO. All rts. reserv.

05499941 **Image available**
PORTABLE INFORMATION RECORDING MEDIUM

PUB. NO.: 09-114741 [JP 9114741 A]
PUBLISHED: May 02, 1997 (19970502)
INVENTOR(s): IRISAWA KAZUYOSHI
APPLICANT(s): DAINIPPON PRINTING CO LTD [000289] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 07-294749 [JP 95294749]
FILED: October 18, 1995 (19951018)
INTL CLASS: [6] G06F-012/14; G06F-012/00; G06K-017/00; G06K-019/073
JAPIO CLASS: 45.2 (INFORMATION PROCESSING -- Memory Units); 45.3 (INFORMATION PROCESSING -- Input Output Units)

ABSTRACT

PROBLEM TO BE SOLVED: To make possible an access with excellent operability, securing sufficient security, for the file having the hierarchical structure for which the separate security setting for every purpose is performed, by performing a specified processing by providing a CPU executing the command imparted from the outside and the first and second memories accessed by this CPU.

SOLUTION: When a command 'SELECT #3 DF 1-2' designating a specified channel and selecting a specified file control area is imparted, unlocking information is maintained as it is for recording parts (1, 3) for which discrimination information is not updated. When other recording parts (2, 2) in which the same discrimination information DF 1 as this updated discrimination is recorded exist for the recording part for which discrimination information is not updated, the unlocking information recorded in these other recording parts is copied as it is. When these other recording parts do not exist, a processing writing the unlocking information showning locking is performed.
?

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平9－114741

(43)公開日　平成9年(1997)5月2日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ			技術表示箇所
Ｇ０６Ｆ	12/14	３１０		Ｇ０６Ｆ	12/14	３１０Ｋ	
	12/00	５３７			12/00	５３７Ａ	
Ｇ０６Ｋ	17/00			Ｇ０６Ｋ	17/00	Ｅ	
	19/073				19/00	Ｐ	

審査請求　未請求　請求項の数5　ＦＤ　(全 18 頁)

(21)出願番号　特願平7－294749

(22)出願日　平成7年(1995)10月18日

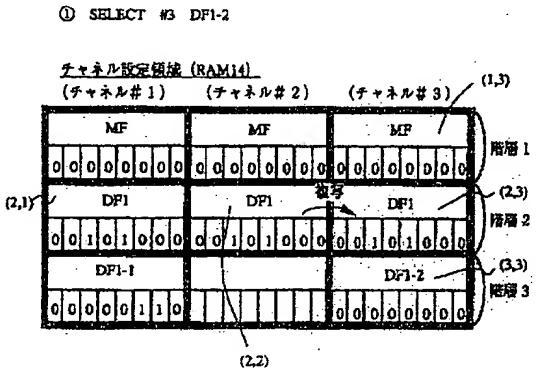
(71)出願人　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目1番1号

(72)発明者　入澤　和義
東京都新宿区市谷加賀町一丁目1番1号
大日本印刷株式会社内

(74)代理人　弁理士　志村　浩

(54)【発明の名称】　携帯可能情報記録媒体

(57)【要約】
【課題】　用途ごとに別々のセキュリティ設定がなされ、階層構造をもったファイルに対し、十分なセキュリティを確保しつつ使い勝手の良いアクセスを行う。
【解決手段】　ＲＡＭ内に、各チャネルごとの開錠状態を示す記録部を各階層ごとに設ける。各チャネル内には、そのチャネルを用いて選択されたファイル管理領域ＤＦへの階層上のパスが記録される。新たにチャネル＃３を用いてＤＦ１－２を選択すると、ＭＦ→ＤＦ１→ＤＦ１－２なるパスが記録されるが、チャネル＃２にも存在するＤＦ１の開錠状態は、チャネル＃３に複写される。いずれかのチャネルにおいてＤＦ１の開錠状態を更新すると、更新された開錠状態が他チャネルのＤＦ１へ複写される。必要に応じて上位階層の開錠状態を参照する旨の設定を行うと、上下両階層の開錠状態のビット間論理和により開錠状態が判断される。



1

【特許請求の範囲】

【請求項１】　外部から与えられるコマンドを実行するＣＰＵと、このＣＰＵによってアクセスされる第１のメモリと第２のメモリと、を備え、前記第１のメモリには、階層構造をもったファイル管理領域を定義して各ファイル管理領域内にそれぞれ所定のファイルを所定のアクセス条件とともに記録し、前記第２のメモリには、前記アクセス条件に関連した開錠情報を記録し、この開錠情報と各ファイルについてのアクセス条件とを比較することにより、前記第１のメモリ内の各ファイルに対するアクセスの可否を判定するようにした携帯可能情報記録媒体において、

前記第２のメモリ内に、複数のチャネル設定領域を設け、各チャネル設定領域を互いに上下の階層関係をもった複数の記録部に分割し、個々の記録部には、特定のファイル管理領域を示す識別情報と、この特定のファイル管理領域についての開錠情報と、を記録できるようにし、

特定のチャネルを指定して特定のファイル管理領域を選択するコマンドが与えられたときには、選択されたファイル管理領域およびこれより上位階層のファイル管理領域の識別情報を、指定されたチャネル設定領域内のそれぞれの階層に対応した記録部に書き込んで記録済状態とし、選択されたファイル管理領域より下位階層に相当する記録部は未記録状態とする書込処理を行い、この書込処理によって、識別情報が更新されなかった記録部については開錠情報をそのまま維持し、識別情報が更新された記録部については、この更新された識別情報と同一の識別情報が記録されている他の記録部が存在する場合には、前記他の記録部に記録されている開錠情報をそのまま複写し、そのような他の記録部が存在しない場合には、未開錠を示す開錠情報を書き込む処理を行い、

特定のチャネルを指定して所定のキー照合を行うコマンドが与えられたときには、指定されたチャネル設定領域内の記録済状態にある最下層の記録部に記録されている開錠情報をキー照合の結果に基いて更新する更新処理を行い、前記最下層の記録部に記録されている識別情報と同一の識別情報が記録されている別な記録部が存在する場合には、前記更新処理によって更新された開錠情報を、前記別な記録部にそのまま複写する処理を行い、

特定のチャネルを指定して所定の対象ファイルをアクセスするコマンドが与えられたときには、指定されたチャネル設定領域内の記録済状態にある最下層の記録部に記録されている識別情報で特定されるファイル管理領域内に前記対象ファイルが所属し、かつ、前記最下層の記録部に記録されている開錠情報が、前記対象ファイルのアクセス条件を満足する場合に、前記対象ファイルに対するアクセスを可能とすることを特徴とする携帯可能情報記録媒体。

【請求項２】　請求項１に記載の携帯可能情報記録媒体において、

各ファイル管理領域について、上位階層のファイル管理領域の開錠情報を参照するか否かの設定を行えるようにし、参照する旨の設定がなされていたときには、上位階層のファイル管理領域の開錠情報と自己の開錠情報とを融合させた融合開錠情報が、対象ファイルのアクセス条件を満足する場合に、前記対象ファイルに対するアクセスを可能とするようにしたことを特徴とする携帯可能情報記録媒体。

【請求項３】　請求項２に記載の携帯可能情報記録媒体において、

第２階層以下の各ファイル管理領域について、最上位階層のファイル管理領域の開錠情報を常に参照する旨の設定が行われていることを特徴とする携帯可能情報記録媒体。

【請求項４】　請求項１～３のいずれかに記載の携帯可能情報記録媒体において、

ファイルに対するアクセスコマンドを、そのアクセスの態様に応じて複数のグループに分け、各ファイルについてのアクセス条件を、各グループごとに設定するようにし、

アクセスコマンドが与えられたときには、このアクセスコマンドが所属するグループについて設定されているアクセス条件を開錠情報と比較するようにしたことを特徴とする携帯可能情報記録媒体。

【請求項５】　請求項１～４のいずれかに記載の携帯可能情報記録媒体において、

最上位階層については、複数のチャネルを代表する単一の記録部のみを設けるようにしたことを特徴とする携帯可能情報記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は携帯可能情報記録媒体、特に、ＣＰＵと、このＣＰＵによってアクセスされるメモリとを備えた記録媒体に関する。

【０００２】

【従来の技術】ＩＣカードに代表される携帯可能情報記録媒体は、磁気カードに代わる次世代の媒体として注目を集めており、最近では、半導体集積回路の小型化、低コスト化のための技術革新により、実社会の種々のシステムにおいてＩＣカードが実用されるに至っている。

【０００３】特に、ＣＰＵを内蔵したＩＣカードは、単なる情報記録媒体としての機能だけではなく、情報処理機能を有するため、高度なセキュリティを必要とする情報処理システムへの利用が期待されている。一般に、ＩＣカードには、ＥＥＰＲＯＭなどの不揮発性メモリが内蔵されており、このＥＥＰＲＯＭ内にファイルとして情報が記録されることになる。しかも、ＥＥＰＲＯＭへのアクセスは、内蔵ＣＰＵによって行われるため、予め所定のアクセス条件を設定しておけば、内蔵ＣＰＵがこの

アクセス条件を満足したと判断したときのみ、ファイルへのアクセスを許可するようにすることができる。通常は、いくつかのキーについての照合をアクセス条件として設定する。すなわち、ＥＥＰＲＯＭ内に予めキーを書き込んでおき、この内部のキーと外部から与えられたキーとを内蔵ＣＰＵで比較照合し、両者が一致した場合に、当該キーが開錠されたものと判断するのである。

【０００４】キーとしては、特定の対象者（たとえば、ＩＣカードの所有者、発行者など）を認証するためのキーや、特定のハードウエア（たとえば、端末装置）を認証するためのキーなどが利用されている。通常は、これらのキーを複数用い、ファイルに対するアクセス条件として、複数のキーの開錠を条件として設定することが多い。すなわち、特定のファイルに対するアクセス条件として、特定のキーの組み合わせが要求されることになる。個々のファイルごとに異なったアクセス条件を設定するために、各ファイルごとにそれぞれディレクトリ領域を設け、このディレクトリ領域内に、開錠を必要とするキーを指定する情報を書き込んでおくのが一般的である。この場合、各ファイルに対するアクセスコマンドが外部から与えられると、内蔵ＣＰＵは、まず、そのアクセス対象ファイルについてのディレクトリ領域を参照し、照合を必要とするキーについての開錠作業が完了している場合に限って、アクセスコマンドの実行を行うことになる。

【０００５】

【発明が解決しようとする課題】ＩＣカードは、磁気カードに比べてデータの記憶容量が大きく、内蔵した不揮発性メモリ内に多数のファイルを記録しておくことができる。しかも、ＥＥＰＲＯＭなどの内蔵不揮発性メモリの容量は、半導体集積回路の製造技術の進歩により、今後も益々増加してゆくものと期待されている。このため、１枚のＩＣカードを複数の用途に利用する利用形態が一般化するものと予想される。たとえば、銀行用カード、クレジットカード、交通機関用プリペイドカード、病院用カード、といった複数の用途に対して、１枚のＩＣカードで対応することが可能になる。

【０００６】このような複数の用途に対応するＩＣカードでは、個々の用途ごとにそれぞれ別個のファイルを用意する必要が生じ、各ファイルに対するアクセス条件もそれぞれ別個独立して設定する必要がある。しかも、用途の異なる複数のファイルを交互にアクセスするような利用形態も、今後は益々増えてゆくものと予想される。たとえば、病院用カードとしての部分に書き込まれた医療費を、銀行用カードとしての部分に書き込まれた預金残高から振り替えることにより、医療費の支払いを行うような場合、病院用ファイルと銀行用ファイルとを交互にアクセスする必要が生じる。この場合、病院用ファイルに対するセキュリティと銀行用カードに対するセキュリティとは、別個に設定されているため、各ファイルをアクセスするごとにそれぞれ開錠操作が必要になり、使い勝手が悪いという問題が生じる。

【０００７】このような多用途に対応したＩＣカードについての使い勝手を向上させる手法として、アクセスチャネルという概念を導入し、個々のアクセスチャネルごとに開錠操作を行う方法が提案されている。たとえば、特開平７－１６０５４７号公報には、各チャネルごとにそれぞれ異なる識別番号を定義し、それぞれのチャネルごとに開錠状態を記録しておく方法が開示されている。しかしながら、階層構造をもったファイルについて、用途ごとに別々のセキュリティが設定されている場合に、種々のファイルを交錯してアクセスするには、十分な使い勝手が得られていないのが現状である。

【０００８】そこで本発明は、用途ごとに別々のセキュリティ設定がなされ、しかも階層構造をもったファイルに対して、十分なセキュリティを確保しつつ使い勝手の良いアクセスが可能な携帯可能情報記録媒体を提供することを目的とする。

【０００９】

【課題を解決するための手段】

(1)　本発明の第１の態様は、外部から与えられるコマンドを実行するＣＰＵと、このＣＰＵによってアクセスされる第１のメモリと第２のメモリと、を備え、第１のメモリには、階層構造をもったファイル管理領域を定義して各ファイル管理領域内にそれぞれ所定のファイルを所定のアクセス条件とともに記録し、第２のメモリには、アクセス条件に関連した開錠情報を記録し、この開錠情報と各ファイルについてのアクセス条件とを比較することにより、第１のメモリ内の各ファイルに対するアクセスの可否を判定するようにした携帯可能情報記録媒体において、第２のメモリ内に、複数のチャネル設定領域を設け、各チャネル設定領域を互いに上下の階層関係をもった複数の記録部に分割し、個々の記録部には、特定のファイル管理領域を示す識別情報と、この特定のファイル管理領域についての開錠情報と、を記録できるようにし、特定のチャネルを指定して特定のファイル管理領域を選択するコマンドが与えられたときには、選択されたファイル管理領域およびこれより上位階層のファイル管理領域の識別情報を、指定されたチャネル設定領域内のそれぞれの階層に対応した記録部に書き込んで記録済状態とし、選択されたファイル管理領域より下位階層に相当する記録部は未記録状態とする書込処理を行い、この書込処理によって、識別情報が更新されなかった記録部については開錠情報をそのまま維持し、識別情報が更新された記録部については、この更新された識別情報と同一の識別情報が記録されている他の記録部が存在する場合には、他の記録部に記録されている開錠情報をそのまま複写し、そのような他の記録部が存在しない場合には、未開錠を示す開錠情報を書き込む処理を行い、特定のチャネルを指定して所定のキー照合を行うコマンド

が与えられたときには、指定されたチャネル設定領域内の記録済状態にある最下層の記録部に記録されている開錠情報をキー照合の結果に基いて更新する更新処理を行い、この最下層の記録部に記録されている識別情報と同一の識別情報が記録されている別な記録部が存在する場合には、更新処理によって更新された開錠情報を、この別な記録部にそのまま複写する処理を行い、特定のチャネルを指定して所定の対象ファイルをアクセスするコマンドが与えられたときには、指定されたチャネル設定領域内の記録済状態にある最下層の記録部に記録されている識別情報で特定されるファイル管理領域内に対象ファイルが所属し、かつ、この最下層の記録部に記録されている開錠情報が、対象ファイルのアクセス条件を満足する場合に、この対象ファイルに対するアクセスを可能とするようにしたものである。

【００１０】(2)　本発明の第２の態様は、上述の第１の態様に係る携帯可能情報記録媒体において、各ファイル管理領域について、上位階層のファイル管理領域の開錠情報を参照するか否かの設定を行えるようにし、参照する旨の設定がなされていたときには、上位階層のファイル管理領域の開錠情報と自己の開錠情報とを融合させた融合開錠情報が、対象ファイルのアクセス条件を満足する場合に、対象ファイルに対するアクセスを可能とするようにしたものである。

【００１１】(3)　本発明の第３の態様は、上述の第２の態様に係る携帯可能情報記録媒体において、第２階層以下の各ファイル管理領域について、最上位階層のファイル管理領域の開錠情報を常に参照する旨の設定を行うようにしたものである。

【００１２】(4)　本発明の第４の態様は、上述の第１～第３に記載の携帯可能情報記録媒体において、ファイルに対するアクセスコマンドを、そのアクセスの態様に応じて複数のグループに分け、各ファイルについてのアクセス条件を、各グループごとに設定するようにし、アクセスコマンドが与えられたときには、このアクセスコマンドが所属するグループについて設定されているアクセス条件を開錠情報と比較するようにしたものである。

【００１３】(5)　本発明の第５の態様は、上述の第１～第４に記載の携帯可能情報記録媒体において、最上位階層については、複数のチャネルを代表する単一の記録部のみを設けるようにしたものである。

【００１４】

【発明の実施の形態】本発明に係る携帯可能情報記録媒体は、外部から与えられるコマンドを実行するＣＰＵと、このＣＰＵによってアクセスされる２種類のメモリとを有する。もっとも、この２種類のメモリは、その記録内容によって概念上区別されるだけのものであり、物理的には単一のメモリ素子を領域分割して用いてもかまわない。これら２種類のメモリのうち、第１のメモリには、この媒体に本来記録すべきファイルが、それぞれ所定のアクセス条件とともに記録される。このアクセス条件は、そのファイルに対するアクセスを行うためには、どのキーを照合する必要があるかを示す条件である。一方、第２のメモリには、このアクセス条件に関連した開錠情報が記録される。具体的には、どのキーの照合が既に完了して開錠状態になっているか、という情報が記録されることになる。したがって、特定のファイルに対する読出コマンドや書込コマンドなどのアクセスコマンドが与えられた場合には、このアクセス対象となったファイルについてのアクセス条件と、その時点における開錠情報とを比較することにより、アクセスの可否が判定される。

【００１５】本発明では、第１のメモリ内に、階層構造をもったファイル管理領域が定義される。このファイル管理領域は、概念的には、いわば具体的なファイルを入れる箱に相当するものであり、この箱を入れ子状にすることにより階層構造を採ることができる。具体的なファイルは、いずれかの箱の中に入れられることになる。セキュリティは、個々の箱ごとに別個に設定することができる。したがって、各用途ごとに別個の箱を用意しておけば、用途ごとに異なるセキュリティ設定が可能になる。

【００１６】第２のメモリ内に記録される開錠情報も、個々の箱ごとに、すなわち、個々のファイル管理領域ごとに別個に記録される。しかも、実際のアクセスは「チャネル」という概念を用いて行われる。すなわち、まず特定のチャネルを指定して、特定のファイル管理領域（箱）を選択する。特定のチャネルについて、どの箱が選択されたかを示すために、第２のメモリ内には、複数のチャネル設定領域が設けられる。各チャネル設定領域は、上下の階層関係をもった複数の記録部に分割され、個々の記録部には、特定のファイル管理領域を示す識別情報と、この特定のファイル管理領域についての開錠情報と、が記録される。特定のチャネルを指定して特定のファイル管理領域（箱）を選択すると、この選択されたファイル管理領域（選択された箱）およびこれより上位階層のファイル管理領域（外側の箱）を示す識別情報が、指定されたチャネル設定領域内のそれぞれの階層に対応した記録部に書き込まれる。このような書き込みが行われた記録部は記録済状態になる。このとき、選択されたファイル管理領域（選択された箱）より下位階層のファイル管理領域（内側の箱）に相当する記録部は未記録状態である。したがって、チャネル設定領域内の記録済の最下層の記録部が、常に、そのチャネルについて選択されたファイル管理領域（選択された箱）に対応することになる。

【００１７】このように、チャネル設定領域には、選択されたファイル管理領域（箱）に至るまでの階層構造上のパスが記録されることになる。各チャネルごとに、それぞれ任意のファイル管理領域を選択することができる

ので、異なるチャネルについて、部分的にパスが共通するファイル管理領域が選択されると、異なる記録部に同一のファイル管理領域を示す識別情報が記録されることになる。

【００１８】各記録部には、ファイル管理領域（箱）を特定するための識別情報とともに、そのファイル管理領域（箱）についての開錠情報が記録される。すなわち、１つの記録部を参照すれば、ある１つの箱についての現時点における開錠状態が認識できることになる。本発明の重要な特徴は、この開錠情報の更新方法にある。各記録部の開錠情報は、次の２とおりの場合に更新される。第１の場合は、特定のチャネルを指定して、特定のファイル管理領域（箱）を選択するコマンドが与えられたときである。この場合は、識別情報が更新されなかった記録部については、開錠情報もそのまま更新されずに維持される。すなわち、既に何らかの開錠操作が行われていた箱については、その開錠情報がそのまま維持されることになり、再度の開錠操作を行う必要はない。一方、識別情報が更新された記録部については、この更新された識別情報と同一の識別情報が記録されている他の記録部が存在する場合には、他の記録部に記録されている開錠情報をそのまま複写する。すなわち、他のチャネルにおいて、同一のファイル管理領域（箱）に対して既に何らかの開錠操作が行われていた場合には、その開錠情報がそのまま複写されるので、別なチャネルで同じファイル管理領域（箱）をアクセスする場合でも、再度の開錠操作を行う必要はなくなる。そして、そのような他の記録部が存在しない場合には、未開錠を示す開錠情報が書き込まれる。すなわち、その選択されたファイル管理領域（箱）について、過去にいずれかのチャネルにおいて開錠操作が行われたという記録が残っていない場合には、未開錠なる開錠情報が書き込まれ、アクセスには所定の開錠操作が要求されることになる。

【００１９】各記録部の開錠情報が更新される第２の場合は、特定のチャネルを指定して所定のキー照合を行うコマンドが与えられたときである。前述したように、各チャネル設定領域内の記録済状態にある最下層の記録部は、常に、そのチャネルについて選択されたファイル管理領域（選択された箱）を示している。別言すれば、チャネルの指定は、最下層の記録部に記録されたファイル管理領域（箱）の指定と同等の意味をもつ。そこで、このようなキー照合コマンドが与えられたときには、そのチャネルの最下層の記録部に記録されたファイル管理領域（箱）についての照合処理が実行され、キー照合が一致すれば、そのキーが開錠状態になったことを示す開錠情報がこの記録部に書き込まれることになる。このように、キー照合コマンドの実行により、この記録部内の開錠情報が更新されることになるが、本発明では、この記録部に記録されている識別情報と同一の識別情報が記録されている別な記録部が存在する場合には、更新処理によって更新された開錠情報を、この別な記録部にもそのまま複写する処理が行われる。すなわち、ある１つのチャネルについて、ある１つのファイル管理領域（箱）の開錠状態に変更があった場合には、別なチャネルに記録されている同一のファイル管理領域（箱）の開錠状態にも同一の変更が加えられることになる。別言すれば、１つのチャネルにおける開錠操作が、別なチャネルにおいても反映されることになり、同一のファイル管理領域（箱）についての開錠操作を、アクセスチャネルが変わるごとに繰り返す必要がなくなる。

【００２０】本発明では、個々のファイルに対するアクセスも、チャネルを指定して行うことになる。このようなアクセスコマンドが与えられると、まず、指定されたチャネル設定領域内の記録済状態にある最下層の記録部に記録されている識別情報で特定されるファイル管理領域（箱）にアクセスの対象となるファイルが所属しているか否かが調べられる。指定されたチャネルによって選択されているファイル管理領域（箱）に、アクセス対象ファイルが所属していなければ、チャネル管轄外のファイルアクセスが行われたことになるので、アクセスは許可されない。アクセス対象ファイルが、チャネルで選択されているファイル管理領域（箱）に所属している場合には、このファイル管理領域（箱）についての開錠情報が、対象ファイルのアクセス条件を満足しているか否かが調べられ、満足している場合には、この対象ファイルに対するアクセスが行われることになる。

【００２１】

【実施例】

§１．　ＩＣカードの基本構成

以下、本発明を図示する実施例に基づいて説明する。図１は、一般的なＩＣカード１０に、外部装置としてのリーダライタ装置２０を接続し、アクセスを行っている状態を示すブロック図である。ＩＣカード１０とリーダライタ装置２０とはＩ／Ｏライン３０によって相互に接続されている。ここで、ＩＣカード１０には、Ｉ／Ｏインタフェース１１、ＣＰＵ１２、ＲＯＭ１３、ＲＡＭ１４、ＥＥＰＲＯＭ１５が内蔵されている。Ｉ／Ｏインタフェース１１は、Ｉ／Ｏライン３０を介してデータを送受するための入出力回路であり、ＣＰＵ１２はこのＩ／Ｏインタフェース１１を介して、リーダライタ装置２０と交信することになる。ＲＯＭ１３内には、ＣＰＵ１２によって実行されるべきプログラムが記憶されており、ＣＰＵ１２はこのプログラムに基いて、ＩＣカード１０を統括制御する機能を有する。ＲＡＭ１４は、ＣＰＵ１２がこのような統括制御を行う上での作業領域として使用されるメモリである。一方、ＥＥＰＲＯＭ１５は、このＩＣカード１０に記録すべき本来のデータを格納するメモリである。

【００２２】このＩＣカード１０に対しては、外部のリーダライタ装置２０から電源やクロックが供給される。

したがって、ＩＣカード１０がリーダライタ装置２０と切り離されると、ＩＣカード１０への電源およびクロックの供給は停止する。しかしながら、ＥＥＰＲＯＭ１５は不揮発性メモリであるため、電源供給が停止した後もその記録内容はそのまま保持される。ただ、ＲＡＭ１４内のデータは、電源供給の停止によりすべて失われる。

【００２３】ＩＣカード１０内の各メモリ１３，１４，１５へのアクセスは、すべてＣＰＵ１２を介して行われ、外部からこれらメモリを直接アクセスすることはできない。すなわち、リーダライタ装置２０からＣＰＵ１２に対して所定の「コマンド」を与えると、ＣＰＵ１２はこの「コマンド」を解釈実行し、その結果を、リーダライタ装置２０に対して「レスポンス」として返送することになる。たとえば、ＥＥＰＲＯＭ１５内の所定のファイルに書き込みを行う場合には、「書込コマンド」とともに書込対象となるデータをＣＰＵ１２に与え、ＣＰＵ１２による「書込コマンド」の実行という形式で書込処理が行われることになる。逆に、ＥＥＰＲＯＭ１５内の所定のファイルからデータの読出しを行う場合は、所定の「読出コマンド」をＣＰＵ１２に与え、ＣＰＵ１２による「読出コマンド」の実行という形式で読出処理が行われることになる。このように、ＩＣカード１０内において「コマンド」の実行が終了すると、実行した「コマンド」に対する「レスポンス」が外部に対して返送される。たとえば、「書込コマンド」を与えた場合には、書込処理が支障なく実行されたか否かを示す「レスポンス」が返送され、「読出コマンド」を与えた場合には、読出対象となったデータがレスポンスという形で返送されることになる。

【００２４】ただし、上述のようなＥＥＰＲＯＭ１５へのアクセスは、無条件で行われるわけではなく、所定のアクセス条件が満足されることが前提となる。このアクセス条件は、個々のファイルごとに、また、個々のコマンドグループごとに設定される。これについては後述する。

【００２５】ＥＥＰＲＯＭ１５内には、階層構造をもったファイル管理領域が定義される。既に述べたように、このファイル管理領域は、概念的には、いわば具体的なファイルを入れる箱に相当するものであり、一般的には、このファイル管理領域は「Dedicated File」と呼ばれている。そこで本実施例では、このファイル管理領域を「ＤＦ」なる記号で示すことにし、特に、最上階層のファイル管理領域を「Master File」の意味を示す記号「ＭＦ」で表すことにする。図２は、階層構造をもった具体的なファイル管理領域を、ＥＥＰＲＯＭ１５内に定義した状態を示す概念図である。最上階層に相当する階層１には、ファイル管理領域ＭＦが定義され、その中に、階層２に相当するファイル管理領域ＤＦ１，ＤＦ２が定義され、それぞれの中に、階層３に相当するファイル管理領域ＤＦ１－１，ＤＦ１－２，ＤＦ２－１，ＤＦ２－２が定義されている。各ファイル管理領域内に示されている円で囲ったＤおよびＫは、それぞれ具体的なデータファイルおよびキーファイルを示す。各ファイル管理領域が「箱」であるのに対し、データファイルＤおよびキーファイルＫは、具体的な情報をもったファイルである。データファイルＤは、本来記録すべきデータを収容したファイルであり、キーファイルＫは、セキュリティ管理のために用いられるキー暗証コードを収容したファイルである。

【００２６】図３は、図２に示すファイル管理領域および各ファイルの階層構造を示すツリー図である。四角で囲ったブロックはいずれもファイル管理領域（箱）を示し、楕円で囲ったブロックは個々のデータファイル（頭に記号Ｄのついたファイル）およびキーファイル（頭に記号Ｋのついたファイル）を示す。説明の便宜上、この図３では、個々のデータファイルおよびキーファイルを特定するために、Ｋ１１，Ｄ１１２などの番号を付して示してある。たとえば、ファイルＫ００，Ｋ０１，Ｄ００，Ｄ０１は、階層１のファイル管理領域ＭＦの管理下にあるファイルであり、ファイルＫ１１，Ｋ１２，Ｄ１１，Ｄ１２は、階層２のファイル管理領域ＤＦ１の管理下にあるファイルであり、ファイルＫ１１１，Ｋ１１２，Ｄ１１１，Ｄ１１２は、階層３のファイル管理領域ＤＦ１－１の管理下にあるファイルである。

【００２７】このように、階層をもったファイル管理領域を定義すると、各ファイルを用途ごとに分けて管理することができる。この実施例では、このＩＣカード１０を、銀行用カード兼病院用カードとして利用する場合を述べる。図４は、各ファイル管理領域に、それぞれ大まかな用途を定義した一例を示すブロック図である。階層１のファイル管理領域ＭＦは、このＩＣカード１０全体を統括管理する領域であり、その管理下にあるデータファイルＤ００，Ｄ０１には、たとえば、このＩＣカード１０の所有者の氏名、住所、電話番号などの情報が記録される。これに対し、階層２のファイル管理領域ＤＦ１は、銀行業務を統括管理する領域であり、その管理下にあるデータファイルＤ１１，Ｄ１２には、たとえば、銀行がこのＩＣカード１０の所有者に付与した顧客番号、担保明細、信用情報などが記録される。また、同じ階層２のファイル管理領域ＤＦ２は、病院業務を統括管理する領域であり、その管理下にあるデータファイルＤ２１，Ｄ２２には、たとえば、病院がこのＩＣカード１０の所有者に付与した患者番号、血液型、身長、体重、緊急連絡先などの情報が記録される。

【００２８】階層３のファイル管理領域ＤＦ１－１，ＤＦ１－２，ＤＦ２－１，ＤＦ２－２は、階層２の業務を更に細分化した個別の業務を管理する領域である。たとえば、ファイル管理領域ＤＦ１－１は、銀行業務のうちの国内預金を管理する領域であり、その管理下にあるデータファイルＤ１１１，Ｄ１１２には、たとえば、普通

預金あるいは定期預金の口座取引情報が記録される。また、ファイル管理領域ＤＦ１－２は、銀行業務のうちの外国為替を管理する領域であり、その管理下にあるデータファイルＤ１２１，Ｄ１２２には、たとえば、ドル立預金の取引情報や外国送金情報などが記録される。一方、ファイル管理領域ＤＦ２－１は、病院業務のうちの診療データを管理する領域であり、その管理下にあるデータファイルＤ２１１，Ｄ２１２には、たとえば、血液検査、レントゲン検査などの検査情報や、投薬情報などが記録される。また、ファイル管理領域ＤＦ２－２は、病院業務のうちの医療費データを管理する領域であり、その管理下にあるデータファイルＤ２２１，Ｄ２２２には、たとえば、初診料、診察料、健康保険点数などの情報が記録される。

【００２９】§２．　セキュリティの設定方法

さて、図３に示す階層構造では、階層１に４個のファイル、階層２に８個のファイル、階層３に１６個のファイル、がそれぞれ定義されているが、これら各ファイルには、それぞれ独立したアクセス条件が設定されている。図５は、１つのファイルについてのアクセス条件の設定例を示すアクセス条件テーブルである。この実施例では、アクセス条件は、コマンドグループごとに設定されている。すなわち、各ファイルに対するアクセスコマンドは、そのアクセスの態様に応じて複数のグループに分けられる。この実施例では、キー照合を行うコマンドの集合であるコマンドグループ０と、情報の読出しを行うコマンドの集合であるコマンドグループ１と、情報の追記を行うコマンドの集合であるコマンドグループ２と、情報の書換え／消去を行うコマンドの集合であるコマンドグループ３と、の４つのグループが定義されている。ただ、コマンドグループ０は、無条件でアクセス可能という設定がなされているため、アクセス条件は、コマンドグループ１～３の３つのコマンドグループについてのみ設定されている。

【００３０】図５に示すアクセス条件は、各コマンドグループのコマンドを実行するために、開錠が必要とされるキーを特定するテーブルから構成されている。すなわち、このアクセス条件テーブルは、各コマンドグループごとに８ビットの情報からなり、各ビットは、キーＫ１～Ｋ８までの８種類のキーについて、それぞれ開錠が必要であるか否かを示している。具体的には、ビット“１”は開錠必要を示し、ビット“０”は開錠不要を示す。たとえば、図５に示すようなアクセス条件が設定されたファイルに対して、情報の読出しを行うコマンドを実行する場合には、コマンドグループ１においてビット“１”が設定されている２つのキーＫ３，Ｋ５についての開錠が行われていなければならない。

【００３１】図５に示すアクセス条件テーブルには、更に、Ｒと記された９番目のビットが設けられているが、この９番目のビットは、上位階層の開錠情報の参照の有無を示す参照ビットである。すなわち、この参照ビットＲに“１”が設定されていると、上位階層の開錠情報を参照することを意味し、“０”が設定されていると、上位階層の開錠情報を参照しないことを意味する。この参照ビットＲの取り扱いについては、後に詳述する。

【００３２】既に述べたように、図５に示すようなアクセス条件テーブルは、図３に楕円で示したすべてのファイル（データファイルおよびキーファイル）について、それぞれ設定されており、これらの各ファイルは、このアクセス条件テーブルとともに、ＥＥＰＲＯＭ１５に書き込まれていることになる。より具体的には、各ファイルには、それぞれ対応するディレクトリ領域が設けられ、このディレクトリ領域内に、各ファイルの先頭アドレスやファイル長が記録されるとともに、アクセス条件テーブルが記録されることになる。

【００３３】一方、ＲＡＭ１４内には、開錠情報が記録される。この開錠情報は、図５に示すアクセス条件テーブルの各キーについて、開錠されたか否かを示すものであり、たとえば、図６(a) に示すような８ビットの領域がＲＡＭ１４内に確保される。この８ビットの領域は、それぞれキーＫ１～Ｋ８の開錠状態を示しており、ビット“１”は開錠、ビット“０”は未開錠を示す。既に述べたように、ＩＣカード１０をリーダライタ装置２０に接続すると、電源やクロックの供給が行われ、ＲＡＭ１４の記録内容はリセット状態となる。図６(a) に示す８ビットの開錠情報は、このリセット時において「００００００００」の状態、すなわち、キーＫ１～Ｋ８のいずれもが未開錠の状態となる。たとえば、キー照合コマンド「ＶＥＲＩＦＹ　Ｋ３　????」をリーダライタ装置２０からＩＣカード１０に与えると（????の部分には、具体的なキー暗証コードがくる）、ＣＰＵ１２は、所定のキーファイルからキーＫ３に対応するキー暗証コードを読出し、これを外部から与えられたキー暗証コード「????」と比較照合し、両者が一致していれば、図６(b) に示すように、ＲＡＭ１４内の開錠情報の第３ビットＫ３にビット“１”を書き込み、キーＫ３が開錠状態になったことを示す。続いて、キー照合コマンド「ＶＥＲＩＦＹ　Ｋ５　????」を与えて照合を行えば、図６(c)に示すように、ＲＡＭ１４内の開錠情報の第５ビットＫ５にもビット“１”が書き込まれる。こうして、２つのキーＫ３，Ｋ５が開錠状態になれば、図５に示すようなアクセス条件が設定されているファイルに対して、コマンドグループ１に属するコマンドの実行が可能になる。

【００３４】以上、ＲＡＭ１４内の開錠情報に基くアクセス可否判定の基本原理を述べたが、本発明の特徴のひとつは、このＲＡＭ１４内の開錠情報を、チャネルごとに、階層ごとに記録する点にある。すなわち、本発明では、ＲＡＭ１４内の開錠情報は、図６に示すような単純な構成で記録されるのではなく、図７に示すような構成

をもったチャネル設定領域をＲＡＭ１４内に設定し、このチャネル設定領域内に記録されることになる。この図７に示す例では、３つのチャネル設定領域（チャネル＃１，＃２，＃３）が定義されており、各チャネル設定領域は、互いに上下の階層関係をもった３つの記録部に分割されている。すなわち、３つのチャネル設定領域のそれぞれが、階層１～３の３つの記録部に分割され、合計９個の記録部が形成されている。ここで各記録部には、特定のファイル管理領域を示す識別情報を記録する領域（上段）と、この特定のファイル管理領域についての開錠情報を記録する領域（８区画に分割された下段）と、が設けられている。この下段の記録領域には、図６に示したような８ビットからなる開錠情報が記録され、この開錠情報と、図５に示したアクセス条件テーブルとを比較して、アクセスの可否判定が行われることになる。

【００３５】§３．　具体的な利用態様を示す実施例

続いて、上述したＩＣカードの具体的な利用態様を、図７に示すチャネル設定領域の記録内容の変遷を追いながら説明する。この実施例では、ＩＣカード１０をリーダライタ装置２０に接続した直後のリセット時には、ＲＡＭ１４内のチャネル設定領域の記録内容は、図８に示すような初期状態になる。すなわち、各記録部上段には、識別情報が未記録であることを示す「ＦＦＦＦ」なる２バイトのデータが書き込まれ、各記録部下段には、８個のキーすべてが未開錠であることを示す「００００００００」なる１ビットのデータが書き込まれる。なお、以下の説明では、便宜上、この９個の記録部を図８に示すように、記録部（１，１），記録部（１，２），…，記録部（３，３）と呼ぶことにする。

【００３６】＜３－１：ファイル管理領域の選択その１＞本発明では、各ファイルをアクセスする準備段階として、特定のチャネルを指定して特定のファイル管理領域を選択する作業が必要になる。この作業を行うためには、リーダライタ装置２０からＩＣカード１０に対して、所定のフォーマットをもった選択コマンドを与えればよい。ここでは、たとえば、図９①に示すように、「ＳＥＬＥＣＴ　＃１　ＤＦ１」なるフォーマットで、選択コマンドを与えた場合を考える。この選択コマンドは、特定のチャネル＃１を指定して、特定のファイル管理領域ＤＦ１を選択するコマンドである。このようなコマンドが与えられると、ＣＰＵ１２は、選択されたファイル管理領域ＤＦ１およびこれより上位階層のファイル管理領域ＭＦの識別情報を、指定されたチャネル設定領域（チャネル＃１）内のそれぞれの階層に対応した記録部の上段に書き込んで記録済状態とし、各記録部の下段にはすべてのキーが未開錠であることを示す開錠情報を書き込む処理を行う。図９は、このような処理が行われた直後のチャネル設定領域の状態を示している。各記録部の上段には、実際には、特定のファイル管理領域を示す２バイトの識別情報が書き込まれるが、図では、説明の便宜上、各ファイル管理領域名（ＭＦ，ＤＦ１）を直接書き込んだ状態を示してある。また、図が繁雑になるのを避けるため、説明に直接関連しない未記録状態の記録部は空欄にして示すことにするが、実際には、これらの空欄には、図８に示すように、「ＦＦＦＦ（上段）」もしくは「００００００００（下段）」なるデータが書き込まれている。

【００３７】結局、各チャネル設定領域を構成する記録部のうち、上段が「ＦＦＦＦ」である記録部は未記録状態の記録部を示し、上段が「ＦＦＦＦ」以外である記録部は記録済状態の記録部を示す。そして、各チャネル設定領域において、記録済状態にある最下層の記録部に識別情報が記録されているファイル管理領域が、当該チャネルについて現在選択されているファイル管理領域となる。図９に示す例の場合、チャネル＃１の領域において、記録済状態にある最下層の記録部（２，１）には、ファイル管理領域ＤＦ１を示す識別情報が書き込まれているので、チャネル＃１について現在選択されているファイル管理領域は、ＤＦ１ということになる。このとき、チャネル＃１の上位階層の記録部（１，１）には、ファイル管理領域ＭＦの識別情報が書き込まれているが、これは、現在選択されているファイル管理領域ＤＦ１の階層構造上の親がＭＦであることを示す役目を果たすとともに、後述するように、上位階層の開錠情報を参照する設定を可能にするためのものである。

【００３８】本発明では、このように特定のチャネルを指定して特定のファイル管理領域を選択するコマンドが与えられたときには、選択されたファイル管理領域およびこれより上位階層のファイル管理領域の識別情報が、指定されたチャネル設定領域内のそれぞれの階層に対応した記録部に書き込まれ、選択されたファイル管理領域より下位階層に相当する記録部は未記録状態とされる。したがって、たとえば、図９①に示す「ＳＥＬＥＣＴ　＃１　ＤＦ１」なる選択コマンドの代わりに、図１０①に示す「ＳＥＬＥＣＴ　＃１　ＤＦ１－２」なる選択コマンドを与えて、階層３のファイル管理領域ＤＦ１－２を選択した場合には、チャネル＃１の記録内容は図１０に示すようなものになる。この図１０では、記録済状態にある最下層の記録部（３，１）には、ファイル管理領域ＤＦ１－２を示す識別情報が書き込まれているので、チャネル＃１について現在選択されているファイル管理領域は、ＤＦ１－２ということになる。

【００３９】＜３－２：キーの照合その１＞続いて、キーの照合が行われた場合の、チャネル設定領域の更新処理を説明する。本発明では、キーの照合は、特定のチャネルを指定して所定のキー照合を行うコマンドを与えることによって行われる。たとえば、いま、図９に示すように、チャネル＃１としてファイル管理領域ＤＦ１が選択されている状態において、この選択されているファイル管理領域ＤＦ１についてのキー照合を行う場合を考え

る。ここでは、キーＫ３とキーＫ５の照合を行うものとしよう。この場合、まず、図１１①に示すような「ＶＥＲＩＦＹ　＃１　Ｋ３　？？？？」なる照合コマンドを与えればよい。ここで、「？？？？」は具体的なキー暗証コードであり、ＣＰＵ１２は、チャネル＃１として選択されているファイル管理領域ＤＦ１内の所定のキーファイルから、キーＫ３の暗証コードを読出し、これを外部から与えられたキー暗証コード「？？？？」と比較照合する。そして、両者が一致すれば、図１１の記録部（２，１）の下段第３ビット目に開錠状態を示すビット"１"を書き込む処理を行う。続いて、図１１②に示すような「ＶＥＲＩＦＹ　＃１Ｋ５　？？？？」なる照合コマンドが与えられたら、キーＫ５の照合を行い、一致すれば、第５ビット目にビット"１"を書き込む処理を行う。図１１に示す記録部（２，１）のビット状態は、このような処理が行われた直後の状態を示している。

【００４０】結局、本発明において、特定のチャネルを指定して所定のキー照合を行うコマンドが与えられた場合には、指定されたチャネル設定領域内の記録済状態にある最下層の記録部（上述の例の場合は、記録部（２，１））に記録されている開錠情報を、キー照合の結果に基いて更新する更新処理が行われることになる。

【００４１】＜３－３：ファイルのアクセス＞本発明におけるファイルのアクセスは、特定のチャネルを指定して所定の対象ファイルをアクセスするコマンドを与えることによって行われる。たとえば、図４に示すような用途が定義されている状態において、銀行業務全般に用いるデータ（たとえば、顧客番号）を、ファイル管理領域ＤＦ１の管理下にあるデータファイルＤ１１から読み出す処理を行う場合を考えよう。ここでは、より具体的に、データファイルＤ１１内の第８レコードを読み出すことにする。本発明では、このように特定のファイルをアクセスする場合も、必ず特定のチャネルを指定する必要がある。しかも、指定するチャネルは、アクセス対象ファイルを管理するファイル管理領域を現在選択中のチャネルでなければならない。別言すれば、特定のファイルをアクセスするコマンドを与える前には、必ず、そのアクセス対象ファイルを管理するファイル管理領域を特定のチャネルを用いて選択しておく必要がある。

【００４２】上述の実施例の場合、図９①に示す「ＳＥＬＥＣＴ　＃１　ＤＦ１」なる選択コマンドにより、チャネル＃１を用いてファイル管理領域ＤＦ１を選択し、更に、図１１①，②に示す照合コマンドにより、キーＫ３，Ｋ５を開錠状態にしておけば、データファイルＤ１１内の第８レコードを読み出すことが可能になる。具体的には、図１１③に示す「ＲＥＡＤ　＃１　Ｄ１１　ＲＥＣ８」なるアクセスコマンドを与えればよい。ＣＰＵ１２は、このようなファイルアクセスのコマンドを受け取ると、まず、指定されたチャネル設定領域内の記録済状態にある最下層の記録部（この例の場合、記録部（２，１））に記録されている識別情報で特定されるファイル管理領域（この例の場合、ファイル管理領域ＤＦ１）内に、アクセスの対象ファイル（この例の場合、データファイルＤ１１）が所属しているか否かを判断する。もし所属していなかった場合には、アクセス対象ファイルが発見できない旨のエラーレスポンスがリーダライタ装置２０側に伝達される。上述の例の場合、アクセスの対象ファイルＤ１１は、ファイル管理領域ＤＦ１内に所属しているファイルとして発見されるので、エラーは生じない。

【００４３】アクセス対象のファイルが発見されたら、続いて、アクセス条件が満たされているか否かの判定が行われる。すなわち、ＣＰＵ１２は、指定されたチャネル設定領域内の記録済状態にある最下層の記録部（この例の場合、記録部（２，１））に記録されている開錠情報（この例の場合、「００１０１０００」）と、アクセス対象のファイルについて設定されているアクセス条件（たとえば、図５に示すようなアクセス条件テーブル）と、を比較し、アクセス条件が満足されているか否かを判断するのである。この例の場合、「ＲＥＡＤ」なるコマンドは、コマンドグループ１に所属する読出しコマンドであるから、図５のアクセス条件テーブルによれば、キーＫ３およびＫ５が開錠状態になっていれば、アクセス可能である。図１１に示す記録部（２，１）の開錠情報は、この条件を満たしている。よって、データファイルＤ１１に対するアクセスは許可され、第８レコードの内容がリーダライタ装置２０側へ読み出されることになる。

【００４４】＜３－４：ファイル管理領域の選択その２＞図１１に示す状態では、チャネル＃１を用いてファイル管理領域ＤＦ１が選択状態となっているので、チャネル＃１を指定したアクセスコマンドでは、ファイル管理領域ＤＦ１の管理下にあるファイルしかアクセスすることはできない。たとえば、ここで、外国為替に関する処理を行うために、ファイル管理領域ＤＦ１－２の管理下にあるデータファイルＤ１２１をアクセスする必要が生じたものとしよう。この場合、新たに、ファイル管理領域ＤＦ１－２を選択しなおす必要がある。そこで、図１２①に示すような選択コマンド「ＳＥＬＥＣＴ　＃１　ＤＦ１－２」を与えたとする。すると、チャネル設定領域の状態は、図１２に示すようになる。図１２と図１１との相違点は、図１２では、新たに記録部（３，１）が記録済状態になっている点である。ここで留意すべき点は、図１１における記録部（２，１）の開錠状態が、図１２においてもそのまま維持されている点である。

【００４５】この留意点は、図１２と図１０とを比較すればより明確になる。図１０は、図８に示す初期状態において「ＳＥＬＥＣＴ　＃１　ＤＦ１－２」なる選択コマンドを与えた状態を示すのに対し、図１２は、図１１に示す中途状態において「ＳＥＬＥＣＴ　＃１　ＤＦ１

－2」なる同じ選択コマンドを与えた状態を示す。別言すれば、図10に示す状態は、何もない初期状態からファイル管理領域DF1－2に至るまでの階層上のパスを定義した場合に得られる状態であるのに対し、図12に示す状態は、図11に示すように、ファイル管理領域DF1に至るまでの階層上のパスを更に階層3のファイル管理領域DF1－2まで伸ばした場合に得られる状態であると言える。このようにパスを伸ばした場合には、伸ばした部分についての開錠状態は、未開錠を示す「00000000」が設定されるが、もとの部分についての開錠状態はもとの状態がそのまま維持されることになる。

【0046】要するに、所定のチャネルを用いてファイル管理領域を選択する選択コマンドが実行された場合、識別情報が更新されなかった記録部（図12の例の場合、記録部（1，1）および記録部（2，1））については開錠情報をそのまま維持し、識別情報が更新された記録部（図12の例の場合、記録部（3，1））については未開錠を示す開錠情報「00000000」を書き込む処理が実行されることになる。

【0047】＜3－5：上位階層の開錠情報の参照＞さて、図12に示す状態では、チャネル#1を用いてファイル管理領域DF1－2が選択されているので、このファイル管理領域DF1－2に対するキー照合処理を行い、必要な開錠操作を行えば、ファイル管理領域DF1－2の管理下にあるデータファイルD121に対するアクセスが許可されることになる。たとえば、データファイルD121からデータを読み出すためのアクセス条件として、3つのキーK3，K5，K6の開錠が要求されていたとしよう。この場合、図13①の「VERIFY #1 K3 ????」、図13②の「VERIFY #1 K5 ????」、図13③の「VERIFY #1 K6 ????」なるキー照合コマンドを与えて開錠操作を行えば、チャネル設定領域は図13に示すような状態となり、記録部（3，1）に、3つのキーK3，K5，K6が開錠状態となったことが記録される。そこで、更に、図13④の「READ #1D121 REC5」なるアクセスコマンドを与えれば、アクセス条件は満足されているため、データファイルD121の第5レコードがリーダライタ装置20側に読み出されることになる。

【0048】しかしながら、図11①，②において、既にキーK3，K5の照合は完了しているので、図13①，②におけるキーK3，K5の照合処理は、冗長な処理操作となっている。実用上は、このように階層間で同一のキー照合をアクセス条件に設定することが少なくない。たとえば、図4に示すように、銀行業務全般を管理するファイル管理領域DF1においては、銀行顧客認証キーK3と銀行支店認証キーK5との照合をアクセス条件として設定し、その下位階層のファイル管理領域DF1－2においては、これらのキー照合に加えて、更に外国為替取扱権限キーK6の照合を付加的なアクセス条件として設定するというような利用形態は、実用上、多用される利用形態である。このような場合、ファイル管理領域DF1のアクセス時に既にキーK3，K5の照合が完了しているのであれば、続いてファイル管理領域DF1－2をアクセスする時には、キーK6の照合を行うだけで十分である。図5のアクセス条件テーブルにおいて示した参照ビットRは、このような便宜を考えて設けたものである。

【0049】たとえば、データファイルD121に対して読出しコマンドを実行するためのアクセス条件テーブルの参照ビットRが、ビット“1”（参照する）に設定されていた場合には、図13①～④の代わりに、図14①，②の2つのコマンドを与えるだけで、データファイルD121の第5レコードがリーダライタ装置20側に読み出されることになる。この場合、ファイル管理領域DF1－2を選択した状態でのキー照合は、キーK6についてのみ行われ、記録部（3，1）の開錠情報は、図14に示すように、キーK6のビットのみが“1”（開錠状態）となる。しかしながら、上位階層の開錠情報（この例の場合、記録部（2，1）の開錠情報）が参照されるので、ファイル管理領域DF1－2の開錠情報は、その上位階層のファイル管理領域DF1の開錠情報「00101000」と自己の開錠情報「00000100」とを融合させた融合開錠情報「00101100」（この実施例の場合、融合開錠情報は個々の開錠情報の各ビットごとの論理和をとることにより得られる）として取り扱われることになり、アクセス条件は満足されていると判断されることになる。

【0050】このように、上位階層の開錠情報を参照できる旨の設定を行っておけば、冗長な照合処理を省略することができ、十分なセキュリティを確保しつつ使い勝手の良いアクセスが可能になる。もちろん、高度なセキュリティを必要とするファイルに対しては、参照ビットRを“0”とし、参照を行わないような設定にしておけばよい。

【0051】＜3－6：ファイル管理領域の選択その3＞さて、外国為替に関するデータファイルD121のアクセスが完了した後に、銀行業務一般用のデータファイルD11を再度アクセスする必要が生じた場合を考えよう。この場合、データファイルD11を管理するファイル管理領域DF1を再度選択しなければならない。それには、図15①に示すように、「SELECT #1 DF1」なる選択コマンドを実行すればよい。これにより、チャネル設定領域は図15に示す状態に更新される。図14と図15とを比較すればわかるように、図15では、記録部（3，1）が初期状態（未記録状態）に戻されている。このように階層3を未記録状態にすれば、記録済状態にある最下層の記録部（2，1）には、

ファイル管理領域ＤＦ１の識別情報が書き込まれているので、現時点で、チャネル＃１はファイル管理領域ＤＦ１を選択している状態に戻ることになる。

【００５２】このように、特定のファイル管理領域の選択を行った場合、選択されたファイル管理領域より下位階層に相当する記録部は未記録状態となり、開錠情報は未開錠を示す「００００００００」となる点は留意すべきである。このように、下位階層のファイル管理領域を選択していた状態から、その上位階層のファイル管理領域を選択する状態に移行した場合に、下位階層の開錠情報を初期状態（未開錠状態）に戻すことは、セキュリティを確保する上で重要である。一般に、階層構造をもったファイル管理領域を構築した場合、下位階層へゆくに従って、より高度なセキュリティが要求される。したがって、上位階層へ戻った場合には、下位階層についての開錠情報を初期状態に戻し、再び下位階層へのアクセスを行う場合には、再度の開錠操作が要求されるようにしておくのが、セキュリティ確保の上からは好ましい。

【００５３】＜３－７：ファイル管理領域の選択その４＞上述したように、選択ファイル管理領域を上位階層に戻した場合、下位階層の開錠情報は未開錠状態に戻される。すなわち、図１４から図１５への変遷により、記録部（３，１）の情報は失われることになる。このような処理は、セキュリティを確保する上では好ましいが、使い勝手の良いアクセスを行う上では障害となる。たとえば、データファイルＤ１１とＤ１２１とを交互にアクセスする必要が生じた場合、ファイル管理領域ＤＦ１とＤＦ２－１とを交互に選択しなければならないが、上位階層のファイル管理領域ＤＦ１を選択した時点で、図１５に示すように、下位階層のファイル管理領域ＤＦ１－２の開錠情報が失われてしまうため、同じ照合操作を何度も繰り返さなくてはならなくなる。このような弊害を避けるためには、別なチャネルを用いた選択を行えばよい。

【００５４】たとえば、図１４に示す状態において、図１５①の「ＳＥＬＥＣＴ　＃１　ＤＦ１」なる選択コマンドを与える代わりに、図１６①の「ＳＥＬＥＣＴ　＃２ＤＦ１」なる選択コマンドを与えるのである。すると、図１６に示すように、チャネル＃１を用いてファイル管理領域ＤＦ１－２を選択した状態のまま、チャネル＃２を用いてファイル管理領域ＤＦ１を選択することが可能になる。チャネル＃２の各記録部には、選択されたファイル管理領域ＤＦ１およびその上位階層のファイル管理領域ＭＦの識別情報が書き込まれる。

【００５５】ここで留意すべき点は、図１６において、記録部（１，１）内の開錠情報が記録部（１，２）へ複写され、記録部（２，１）内の開錠情報が記録部（２，２）へ複写される点である。この複写処理の意図するところは、１つのチャネルにおいて既に完了している照合処理については、別なチャネルにおいても照合処理を不要にすることである。図１６に示す例では、チャネル＃１においてファイル管理領域ＤＦ１のキーＫ３，Ｋ５の照合処理が既に完了しているが、記録部（２，１）内の開錠情報が記録部（２，２）へ複写されるため、チャネル＃１においてもファイル管理領域ＤＦ１のキーＫ３，Ｋ５の照合処理が既に完了した状態となる。よって、チャネル＃２を用いてファイル管理領域ＤＦ１の管理下にあるファイルＤ１１をアクセスする場合は、キーＫ３，Ｋ５の照合処理をあらためて行う必要はなく、図１６②に示す「ＲＥＡＤ　＃２　Ｄ１１　ＲＥＣ２５」のようなアクセスコマンドを与えることにより、ファイルＤ１１内の第２５レコードの読出しが可能になる。

【００５６】前述したように、特定のファイル管理領域を選択するコマンドが実行されると、チャネル設定領域を構成する各記録部（この例の場合、記録部（１，２）および記録部（２，２））の識別情報が更新されることになるが、この更新された識別情報（この例の場合、ＭＦおよびＤＦ１）と同一の識別情報が記録されている他の記録部（この例の場合、記録部（１，１）および記録部（２，１））が存在する場合には、この他の記録部に記録されている開錠情報をそのまま複写する処理が行われることになる点が、本発明のひとつの特徴である。

【００５７】＜３－８：ファイル管理領域の選択その５＞続いて、図１６に示す状態において、今度は、医療費データに関するデータファイルＤ２２２をアクセスする必要が生じたため、図１７①に示す「ＳＥＬＥＣＴ　＃１　ＤＦ２－２」なる選択コマンドを与えた場合を考える。この場合、チャネル＃１は図１７のように更新されることになる。最上層のＭＦに変わりはないので、記録部（１，１）の記録内容は、開錠情報も含めてそのまま維持されるが、階層２，階層３は識別情報がＤＦ２，ＤＦ２－２に更新され、それぞれの開錠情報は未開錠を示す状態になる。このように、チャネル＃１としては、記録部（２，１）の内容は、ＤＦ１からＤＦ２へと更新されてしまうが、ＤＦ１の情報は記録部（２，２）に複写されているため、チャネル＃１が更新されたとしても、ＤＦ１の開錠情報はチャネル＃２としてそのまま残ることになる。ただし、図１６において記録部（３，１）に記録されていたＤＦ１－２の開錠情報は失われてしまう。

【００５８】ＤＦ１－２の開錠情報をそのまま維持したい場合には、図１７①に示す「ＳＥＬＥＣＴ　＃１　ＤＦ２－２」なる選択コマンドの代わりに、図１８①に示す「ＳＥＬＥＣＴ　＃３　ＤＦ２－２」なる選択コマンドを与えればよい。すると、図１８に示すように、チャネル＃１を用いてファイル管理領域ＤＦ１－２を選択し、チャネル＃２を用いてファイル管理領域ＤＦ１を選択した状態のまま、新たに、チャネル＃３を用いてファイル管理領域ＤＦ２－２を選択することが可能になる。チャネル＃３の各記録部には、選択されたファイル管理

領域ＤＦ２－２およびその上位階層のファイル管理領域ＭＦ，ＤＦ２の識別情報が書き込まれる。この場合もやはり、記録部（１，２）内の開錠情報が記録部（１，３）へと複写される。要するに、この複写処理は、同じ識別情報をもった記録部の開錠情報が常に同一となるようにするための処理と言うことができる。図１８の例では、記録部（１，１），（１，２），（１，３）は、いずれも同一の識別情報「ＭＦ」をもった記録部であるから、開錠情報は「００００００００」と同一となり、記録部（２，１），（２，２）は、いずれも同一の識別情報「ＤＦ１」をもった記録部であるから、開錠情報は「００１０１０００」と同一となっている。複写処理は、このような同一性を維持するための処理である。

【００５９】さて、続いて、医療費データに関するデータファイルＤ２２２をアクセスするために、図１９①に示す「ＶＥＲＩＦＹ　＃３　Ｋ７　？？？？」なる照合コマンドおよび図１９②に示す「ＶＥＲＩＦＹ　＃３　Ｋ８　？？？？」なる照合コマンドを与えることにより、ファイル管理領域ＤＦ２－２のキーＫ７，Ｋ８を開錠した場合を考える。この場合、図１９に示すように、記録部（３，３）には、キーＫ７，Ｋ８が開錠状態になったことが書き込まれる。そこで、図１９③に示す「ＲＥＡＤ　＃３　Ｄ２２２　ＲＥＣ４」なる読出しコマンドを与えれば、データファイルＤ２２２の第４レコード（たとえば、医療費未精算額）がリーダライタ装置２０側へと読み出されることになる。

【００６０】ここで、この医療費未精算額について、国内預金データを示すファイルＤ１１１を書換えて振替精算する処理を行ってみよう。この場合、たとえば、図２０①に示す「ＳＥＬＥＣＴ　＃１　ＤＦ１－１」なる選択コマンドを与え、チャネル＃１を更新すればよい。図２０に示すように、記録部（３，１）の識別情報が、ＤＦ１－２からＤＦ１－１へと更新され、開錠情報は未開錠の状態となる。そこで、図２１①に示す「ＶＥＲＩＦＹ　＃１　Ｋ６　？？？？」なる照合コマンドおよび図２１②に示す「ＶＥＲＩＦＹ　＃１　Ｋ７　？？？？」なる照合コマンドを与えることにより、ファイル管理領域ＤＦ１－１のキーＫ６，Ｋ７を開錠し、図２１③に示す「ＷＲＩＴＥ　＃１　Ｄ１１１　ＲＥＣ８　（ＤＡＴＡ）」なる書込コマンドを与えれば、データファイルＤ１１１の第８レコードに、医療費未精算額を示す（ＤＡＴＡ）が書き込まれることになる。

【００６１】続いて、外国為替処理を行うために、ファイル管理領域ＤＦ１－２を選択する必要が生じたので、図２２①に示す「ＳＥＬＥＣＴ　＃３　ＤＦ１－２」なる選択コマンドを与え、チャネル＃３を更新したとする。すると、図２２に示すように、記録部（１，３）の識別情報はＭＦのままであるが、記録部（２，３）の識別情報はＤＦ１に更新され、記録部（３，３）の識別情報はＤＦ１－２に更新される。こうして更新された記録部の開錠情報は、原則として未開錠の状態となるが、上述した同一性維持を図るため、同じ識別情報をもった記録部が他のチャネルにある場合には、開錠情報の複写処理を行う。図２２の例では、ＤＦ１なる同じ識別情報をもった記録部（２，２）もしくは（２，１）の開錠情報が、記録部（２，３）へと複写されることになる。

【００６２】＜３－９：キーの照合その２＞続いて、図２３①に示すような「ＶＥＲＩＦＹ　＃２　Ｋ８　？？？？」なる照合コマンドにより、ファイル管理領域ＤＦ１についてのキーＫ８を照合する処理を行ったとする。キーＫ８が照合一致すれば、記録部（２，２）の開錠情報は、「００１０１０００」の状態から、「００１０１００１」の状態へと更新され、図２３②に示すような「ＷＲＩＴＥ　＃２　Ｄ１１　ＲＥＣ７　（ＤＡＴＡ）」なる書込コマンドを与えることにより、データファイルＤ１１の第７レコードに（ＤＡＴＡ）が書き込まれることになる。ところで、上述した同一性維持を図るためには、このような開錠情報の更新があった場合にも複写処理を行う必要がある。すなわち、図２３に示すように、記録部（２，２）の開錠情報が更新された場合には、同じＤＦ１なる識別情報をもった記録部（２，１）および（２，３）へ、更新された記録部（２，２）の開錠情報を複写する処理が行われる。

【００６３】このように、複写処理は、選択コマンドによりチャネルが更新された場合だけでなく、照合コマンドにより開錠情報が更新された場合にも行う必要がある。要するに、特定の記録部の開錠情報が更新された場合には、同一の識別情報をもった記録部についても、同様の更新が行われるように複写処理を実行すればよい。

【００６４】§４．　ＣＰＵ１２の行う処理

上述した§３では、本発明に係るＩＣカードの利用形態を、チャネル設定領域の記録内容の変遷を追いながら、具体例に即して説明した。このような利用形態を実現させるためには、結局、ＣＰＵ１２は各コマンドに対して次のような処理を行えばよいことがわかる。

【００６５】＜４－１：選択コマンド＞特定のチャネルを指定して特定のファイル管理領域を選択するコマンド（たとえば、図２２①「ＳＥＬＥＣＴ　＃３　ＤＦ１－２」）が与えられたときには、選択されたファイル管理領域およびこれより上位階層のファイル管理領域の識別情報を、指定されたチャネル設定領域内のそれぞれの階層に対応した記録部に書き込んで記録済状態とし、選択されたファイル管理領域より下位階層に相当する記録部は未記録状態とする書込処理を行う（たとえば、図２２参照）。そして、この書込処理によって、識別情報が更新されなかった記録部（図２２の記録部（１，３））については開錠情報をそのまま維持し、識別情報が更新された記録部については、この更新された識別情報と同一の識別情報（図２２のＤＦ１）が記録されている他の記録部（図２２の記録部（２，２））が存在する場合に

は、この他の記録部に記録されている開錠情報をそのまま複写し、そのような他の記録部が存在しない場合には、未開錠を示す開錠情報を書き込む処理を行う（図２２の記録部（３，３））。

【００６６】＜４－２：照合コマンド＞特定のチャネルを指定して所定のキー照合を行うコマンド（たとえば、図２３①「ＶＥＲＩＦＹ　＃２　Ｋ８　？？？？」）が与えられたときには、指定されたチャネル設定領域内の記録済状態にある最下層の記録部（たとえば、図２３の記録部（２，２））に記録されている開錠情報をキー照合の結果に基いて更新する更新処理を行い、この最下層の記録部に記録されている識別情報と同一の識別情報（ＤＦ１）が記録されている別な記録部（たとえば、図２３の記録部（２，１），（２，３））が存在する場合には、更新処理によって更新された開錠情報を、この別な記録部にそのまま複写する処理を行う。

【００６７】＜４－３：アクセスコマンド＞特定のチャネルを指定して所定の対象ファイルをアクセスするコマンド（たとえば、図１１③「ＲＥＡＤ　＃１　Ｄ１１　ＲＥＣ８」）が与えられたときには、指定されたチャネル設定領域内の記録済状態にある最下層の記録部（たとえば、図１１の記録部（２，１））に記録されている識別情報で特定されるファイル管理領域（ＤＦ１）内にアクセス対象ファイル（Ｄ１１）が所属し、かつ、この最下層の記録部に記録されている開錠情報（「００１０１０００」）が、アクセス対象ファイルのアクセス条件（たとえば、図５のコマンドグループ１の条件）を満足する場合に、アクセス対象ファイルに対するアクセスを可能とする。

【００６８】§５．　その他の実施例

以上、本発明を図示する実施例に基いて説明したが、本発明はこれらの実施例に限定されるものではなく、この他にも種々の態様で実施可能である。たとえば、上述の実施例では、図５に示すアクセス条件テーブルの参照ビットＲを“１”にしておくことにより、上位階層の開錠情報を参照できることを説明した。この参照ビットＲは、上述の実施例では、個々のファイルごとにそれぞれ設定していたが、個々のファイル管理領域ごとに１つの参照ビットＲを設定してもよい。この場合、複数階層にわたって参照が行われることもありうる。たとえば、図３において、ファイル管理領域ＤＦ１－１について「参照する」の設定を行い、更に、ファイル管理領域ＤＦ１についても「参照する」の設定を行っておけば、たとえば、階層３のデータファイルＤ１１１に対するアクセスを行う場合には、ファイル管理領域ＤＦ１－１，ＤＦ１，ＭＦの３つの開錠情報の各ビットごとの論理和をとった融合開錠情報に基いて、アクセス条件の判断が行われることになる。

【００６９】また、上述の実施例では、参照ビットＲのビット状態に応じて、上位階層の開錠情報を「参照する」か「参照しない」かの設定を行っていたが、特定の階層については、常に「参照する」旨の設定を行うことも可能である。たとえば、最上位階層のファイル管理領域ＭＦは、このＩＣカードの記録領域全体を統括管理する領域であり、ＩＣカード１０をリーダライタ装置２０に接続した後、まず第１の照合操作として、カード所有者キーなど基本的なキー照合操作が、このファイル管理領域ＭＦについて行われるのが一般的である。そこで、実用上は、第２階層以下の各ファイル管理領域については、最上位階層のファイル管理領域ＭＦの開錠情報を常に参照する旨の設定を行っておくと便利である。このような設定は、わざわざ参照ビットＲを用いて行う必要はなく、ＲＯＭ１３内のプログラムに、常にファイル管理領域ＭＦの開錠情報を参照するようなルーチンを組み込んでおけばよい。

【００７０】なお、上述の実施例では、説明の便宜上、図７に示すような３×３の配列をもった記録部をＲＡＭ１４内に定義する例を述べたが、実際には、最上位階層は必ずファイル管理領域ＭＦが占めることになるので、最上位階層については、複数のチャネルを代表する単一の記録部のみを用意しておけば足りる。すなわち、図２４に示すように、階層１としては、ファイル管理領域ＭＦ専用の記録部を１つだけ設けておけばよく、この記録部には、開錠情報を記録する領域だけを設けておけば足りる。このような構成にすれば、ファイル管理領域ＭＦ内の開錠情報については、チャネル間での複写処理も不要になる。

【００７１】

【発明の効果】以上のとおり本発明によれば、携帯可能情報記録媒体において、用途ごとに別々のセキュリティ設定がなされ階層構造をもったファイルに対して、十分なセキュリティを確保しつつ使い勝手の良いアクセスが可能になる。

【図面の簡単な説明】

【図１】一般的なＩＣカード１０に、外部装置としてのリーダライタ装置２０を接続し、アクセスを行っている状態を示すブロック図である。

【図２】階層構造をもった具体的なファイル管理領域を、ＥＥＰＲＯＭ１５内に定義した状態を示す概念図である。

【図３】図２に示すファイル管理領域および各ファイルの階層構造を示すツリー図である。四角で囲ったブロックはいずれもファイル管理領域を示し、楕円で囲ったブロックは個々のデータファイル（頭に記号Ｄのついたファイル）およびキーファイル（頭に記号Ｋのついたファイル）を示す。

【図４】各ファイル管理領域に、それぞれ大まかな用途を定義した一例を示すブロック図である。

【図５】ＥＥＰＲＯＭ１５内において、各ファイルについてのアクセス条件の設定例を示すアクセス条件テーブ

ルである。

【図６】ＲＡＭ１４内に確保されるキーＫ１～Ｋ８の開錠状態を示す８ビットの領域を示す図である。

【図７】本発明において用いられるチャネル設定領域の一例を示す図である。

【図８】図７に示すチャネル設定領域の初期状態の記録内容を示す図である。

【図９】図８に示す初期状態において、チャネル＃１を用いてファイル管理領域ＤＦ１を選択するコマンドを実行した状態を示す図である。

【図１０】図８に示す初期状態において、チャネル＃１を用いてファイル管理領域ＤＦ１－２を選択するコマンドを実行した状態を示す図である。

【図１１】図９に示す状態において、ファイル管理領域ＤＦ１に対するキー照合コマンドを実行した状態を示す図である。

【図１２】図１１に示す状態において、チャネル＃１を用いてファイル管理領域ＤＦ１－２を選択するコマンドを実行した状態を示す図である。

【図１３】図１２に示す状態において、ファイル管理領域ＤＦ１－２に対するキー照合コマンドを実行した状態を示す図である。

【図１４】上位階層の開錠状態を参照する処理を説明する図である。

【図１５】図１４に示す状態において、チャネル＃１を用いてファイル管理領域ＤＦ１を再選択するコマンドを実行した状態を示す図である。

【図１６】図１４に示す状態において、チャネル＃２を用いてファイル管理領域ＤＦ１を再選択するコマンドを実行した状態を示す図である。

【図１７】図１６に示す状態において、チャネル＃１を用いてファイル管理領域ＤＦ２－２を選択するコマンドを実行した状態を示す図である。

【図１８】図１６に示す状態において、チャネル＃３を＊

＊用いてファイル管理領域ＤＦ２－２を選択するコマンドを実行した状態を示す図である。

【図１９】図１８に示す状態において、ファイル管理領域ＤＦ２－２に対するキー照合コマンドを実行した状態を示す図である。

【図２０】図１９に示す状態において、チャネル＃１を用いてファイル管理領域ＤＦ１－１を選択するコマンドを実行した状態を示す図である。

【図２１】図２０に示す状態において、ファイル管理領域ＤＦ１－１に対するキー照合コマンドを実行した状態を示す図である。

【図２２】図２１に示す状態において、チャネル＃３を用いてファイル管理領域ＤＦ１－２を選択するコマンドを実行した状態を示す図である。

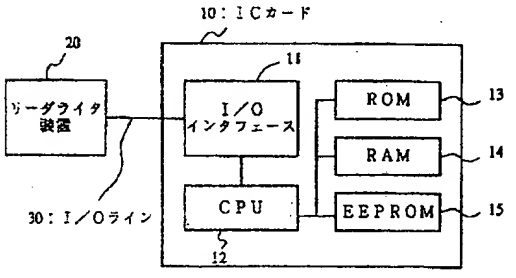
【図２３】図２２に示す状態において、ファイル管理領域ＤＦ１に対するキー照合コマンドを実行した状態を示す図である。

【図２４】最上位階層について、複数のチャネルを代表する単一の記録部のみを用意したチャネル設定領域の一例を示す図である。

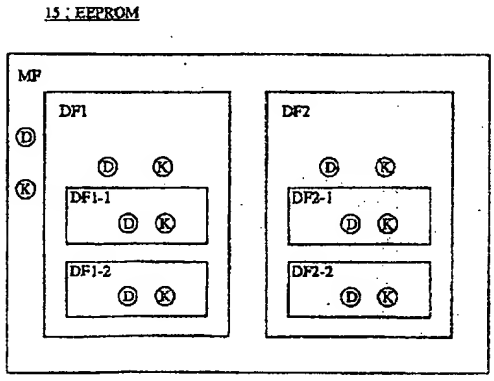
【符号の説明】

１０…ＩＣカード
１１…Ｉ／Ｏインタフェース
１２…ＣＰＵ
１３…ＲＯＭ
１４…ＲＡＭ
１５…ＥＥＰＲＯＭ
Ｄ…データファイル
ＤＦ…ファイル管理領域
Ｋ…キーファイル
Ｋ１～Ｋ８…キー
ＭＦ…最上位階層のファイル管理領域
Ｒ…参照ビット

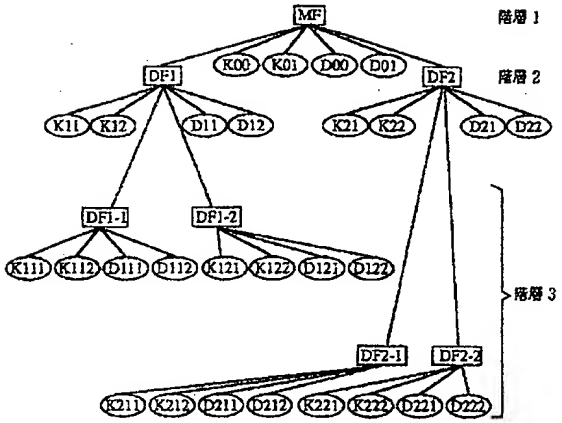
【図１】



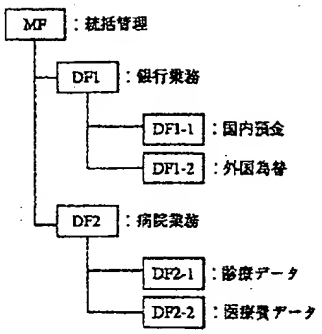
【図２】



【図３】

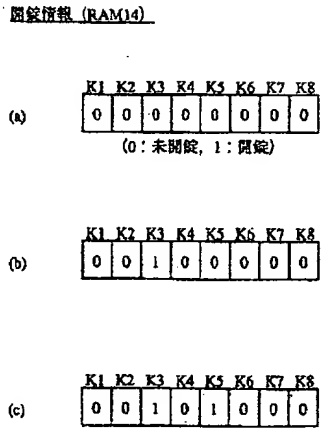


【図４】

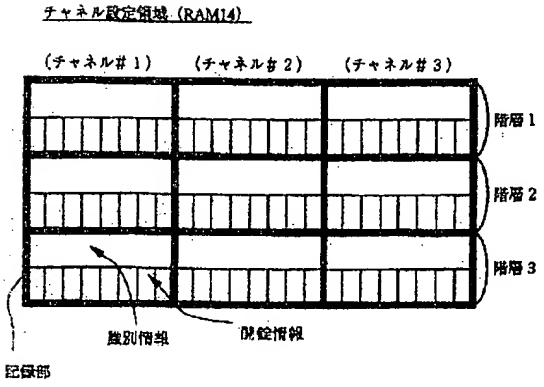


【図５】

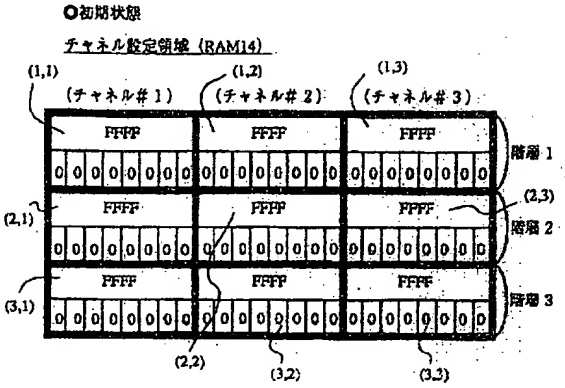
【図６】



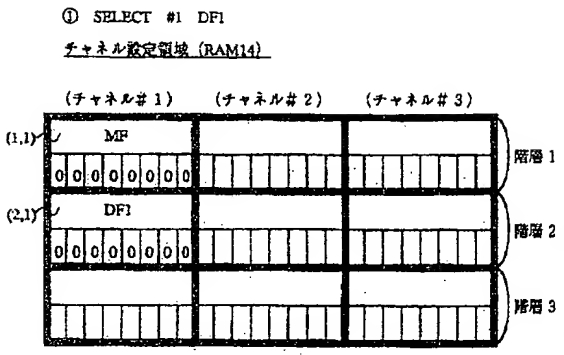
【図７】



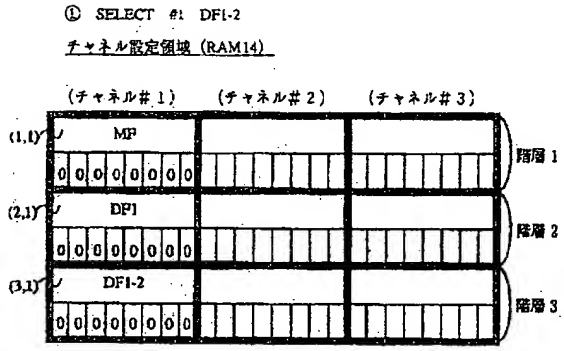
【図８】



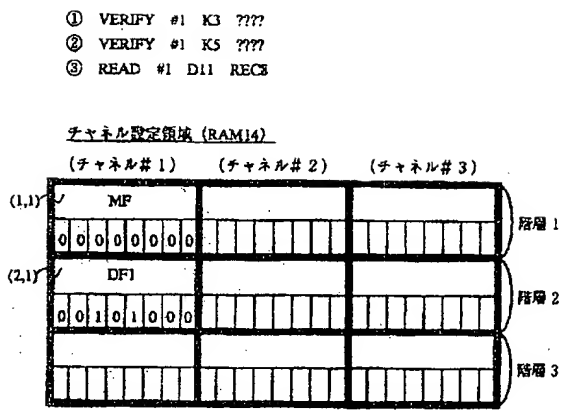
【図９】



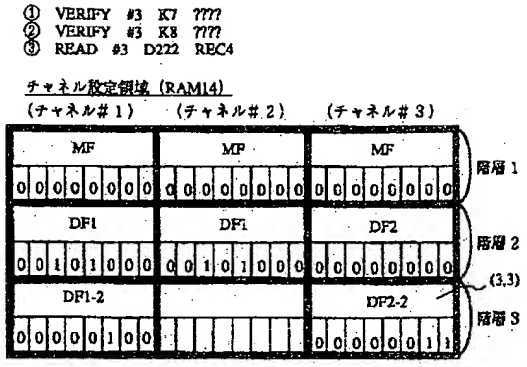
【図１０】



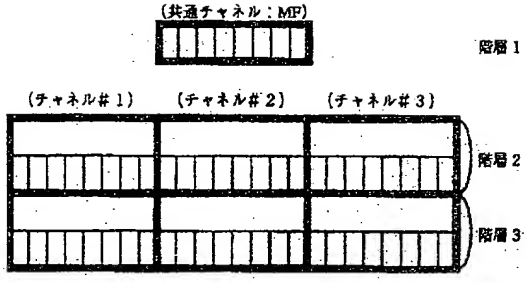
【図１１】



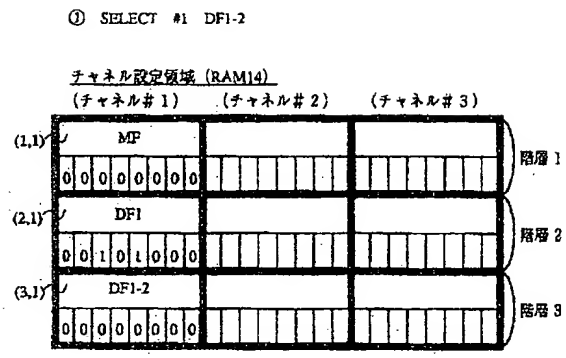
【図１９】



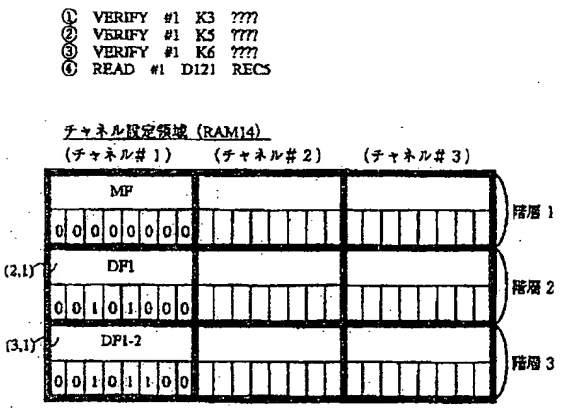
【図２４】



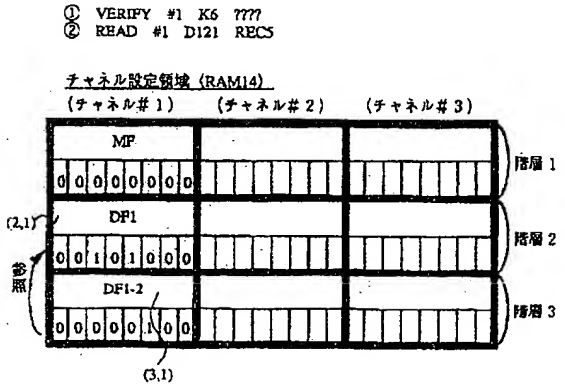
【図１２】



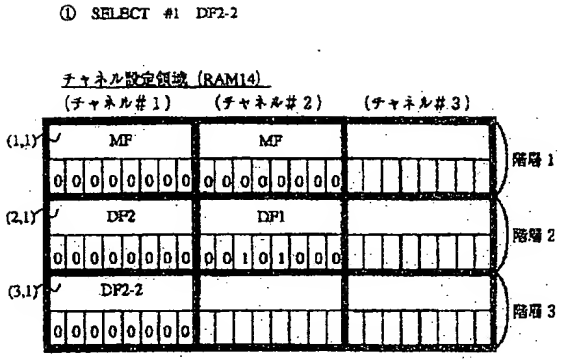
【図１３】



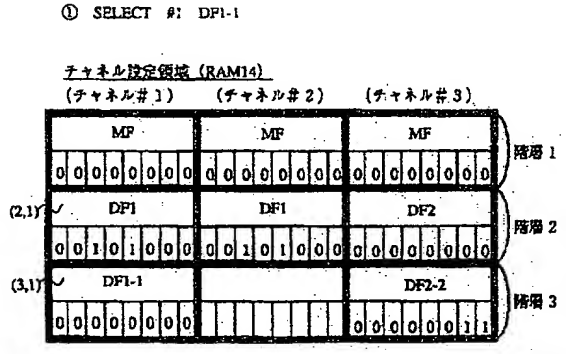
【図１４】



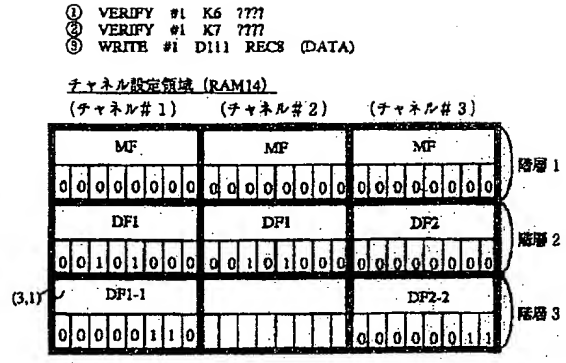
【図１７】



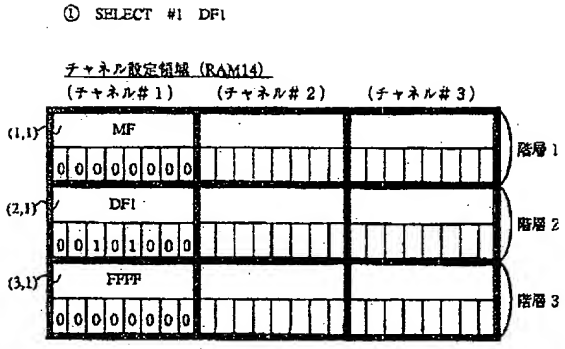
【図２０】



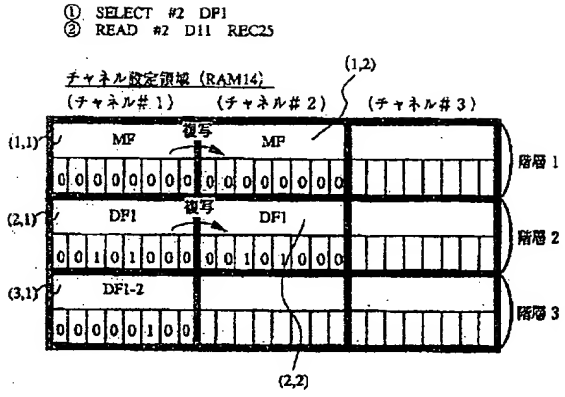
【図２１】



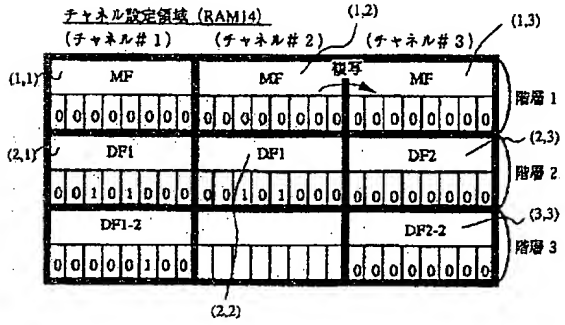
【図１５】



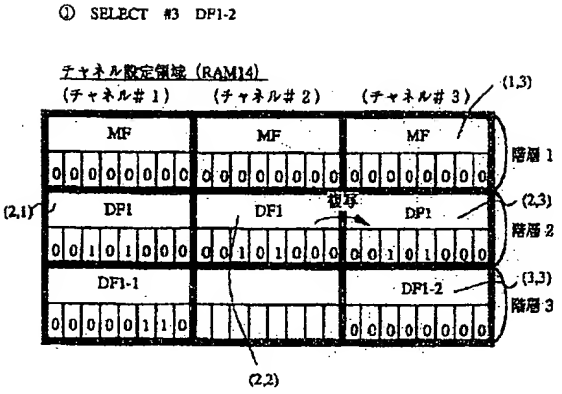
【図１６】



【図１８】



【図２２】



【図２３】